# ACCELERATED MONTGOMERY EXPONENTIATION USING PLURAL MULTIPLIERS


## Abstract of the Disclosure

Montgomery exponentiators and methods modulo exponentiate a generator (g) to a power of an exponent (e). The Montgomery exponentiators and methods include a first multiplier that is configured to repeatedly square a residue of the generator, to produce a series of first multiplier output values at a first multiplier output. A second multiplier is configured to multiply selected ones of the series of first multiplier output values that correspond to a bit of the exponent that is binary one, by a partial result, to produce a series of second multiplier output values at a second multiplier output. By providing two multipliers that are serially coupled as described above, Montgomery exponentiation can be accelerated.